CLAIMS

We claim:

1. A method of detecting an intrusion in a communications network, the method comprising the steps of:

scanning data packets processed by a transport layer of a network protocol associated with said communications network using signatures from a repository of said signatures;

determining if said scanned data packets are malicious; and

taking at least one action if any data packets are determined to be malicious.

2. The method according to claim 1, wherein said at least one action is selected from the group consisting of:

interrupting transmission of any data packets determined to be malicious to said application layer of said network protocol;

logging of errors related to any data packets determined to be malicious;

modifying firewall rules of a host computer if any data packets are determined to be malicious;

informing a network administrator any data packets are determined to be malicious;

intimating said transport layer terminate an existing connection related to any data packets determined to be malicious;

blocking network access to a source of any data packets determined to be malicious;

terminating an application of an application layer if any data packets are determined to be malicious; and

notifying an application of an application layer if any data packets are determined to be malicious.

3. The method according to claim 1, further comprising the step of transmitting to said application layer any data packets determined not to be malicious.

4. The method according to claim 1, wherein said scanning and determining steps are implemented using a scan module.

5. The method according to claim 1, wherein at least one application receive queue (ARQ) functions intermediate said transport layer and said application layer.

6. The method according to claim 7, wherein said scanning step is carried out between said transport layer and said at least one application receive queue (ARQ).

7. The method according to claim 6, further comprising the step of obtaining data from said at least one application receive queue (ARQ).

8. The method according to claim 7, wherein said scanning step is performed on data packets from said at least one application receive queue (ARQ).

9. The method according to claim 1, further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored.

10. The method according to claim 1, wherein said scanning and determining steps are implemented using a scan daemon.

11. The method according to claim 1, further comprising the step of generating fake responses.

12. A method of preventing an intrusion in a communications network, the method comprising the steps of:

disabling a network interface of a host if an idle time expires;

determining if any packets are to be transmitted; and

enabling said network interface if at least one packet is determined to be available to be transmitted.

13. A system for detecting an intrusion in a communications network, the system comprising:

a storage unit for storing data and instructions for a processing unit; and

a processing unit coupled to said storage unit, said processing unit being programmed to scan data packets processed by a transport layer of a network protocol associated with said communications network using signatures from a repository of said signatures, to determine if said scanned data packets are malicious, and to take at least one action if any data packets are determined to be malicious.

14. The system according to claim 13, wherein said at least one action is selected from the group consisting of:

interrupting transmission of any data packets determined to be malicious to said application layer of said network protocol;

logging of errors related to any data packets determined to be malicious;

modifying firewall rules of a host computer if any data packets are determined to be malicious;

informing a network administrator any data packets are determined to be malicious;

intimating said transport layer terminate an existing connection related to any data packets determined to be malicious;

blocking network access to a source of any data packets determined to be malicious;

terminating an application of an application layer if any data packets are determined to be malicious; and

notifying an application of an application layer if any data packets are determined to be malicious.

15. The system according to claim 13, wherein said processing unit is programmed to transmit to said application layer any data packets determined not to be malicious.

16. The system according to claim 13, wherein said processing unit is programmed to implement a scan module.

17. The system according to claim 13, wherein at least one application receive queue (ARQ) functions intermediate said transport layer and said application layer.

18. The system according to claim 17, wherein said scanning is carried out between said transport layer and said at least one application receive queue (ARQ).

19. The system according to claim 17, wherein said processing unit is programmed to obtain data from said at least one application receive queue (ARQ).

20. The system according to claim 19, wherein said scanning is performed on data packets from said at least one application receive queue (ARQ).

21. The system according to claim 13, wherein said processing unit is programmed to dispatch said data packets to one or more handlers for scanning, if said protocol is monitored.

22. The system according to claim 13, wherein said scanning and determining are implemented using a scan daemon.

23. The system according to claim 13, wherein said processing unit is programmed to generate fake responses.

24. A system of preventing an intrusion in a communications network, the system comprising:

a storage unit for storing data and instructions for a processing unit; and

a processing unit coupled to said storage unit, said processing unit being programmed to disable a network interface of a host if an idle time expires, to determine if any packets are to be transmitted, and to enable said network interface if at least one packet is determined to be available to be transmitted.

25. A computer-readable medium containing programmed instructions arranged to detect an intrusion in a communications network, the computer-readable medium comprising:

programmed instructions for scanning data packets processed by a transport layer of a network protocol associated with said communications network using signatures from a repository of said signatures;

programmed instructions for determining if said scanned data packets are malicious; and

programmed instructions for taking at least one action if any data packets are determined to be malicious.

26. The computer-readable medium according to claim 25, wherein said at least one action is selected from the group consisting of:

interrupting transmission of any data packets determined to be malicious to said application layer of said network protocol;

logging of errors related to any data packets determined to be malicious;

modifying firewall rules of a host computer if any data packets are determined to be malicious;

informing a network administrator any data packets are determined to be malicious;

intimating said transport layer terminate an existing connection related to any data packets determined to be malicious;

blocking network access to a source of any data packets determined to be malicious;

terminating an application of an application layer if any data packets are determined to be malicious; and

notifying an application of an application layer if any data packets are determined to be malicious.

27. The computer-readable medium according to claim 25, further comprising programmed instructions for transmitting to said application layer any data packets determined not to be malicious.

28. The computer-readable medium according to claim 25, wherein said programmed instructions for scanning and determining are implemented using a scan module.

29. The computer-readable medium according to claim 25, wherein at least one application receive queue (ARQ) functions intermediate said transport layer and said application layer.

30. The computer-readable medium according to claim 29, wherein said scanning is carried out between said transport layer and said at least one application receive queue (ARQ).

31. The computer-readable medium according to claim 25, further comprising programmed instructions for obtaining data from said at least one application receive queue (ARQ).

32. The computer-readable medium according to claim 31, wherein said scanning is performed on data packets in said at least one application receive queue (ARQ).

33. The computer-readable medium according to claim 25, further comprising programmed instructions for dispatching said data packets to one or more handlers for scanning, if said protocol is monitored.

34. The computer-readable medium according to claim 25, wherein said scanning and determining are implemented using a scan daemon.

35. A computer-readable medium of preventing an intrusion in a communications network, the computer-readable medium comprising:

programmed instructions for disabling a network interface of a host if an idle time expires;

programmed instructions for determining if any packets are to be transmitted; and

programmed instructions for enabling said network interface if at least one packet is determined to be available to be transmitted.